



Received & Inspected

MAR - 3 2008

FCC Mail Room

February 29, 2008

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, SW, Suite TW-A325
Washington, DC 20554.

RE: CPNI Certifications for 2007
EB Docket No. 06-36

Dear Ms. Dortch:

Enclosed, please find certifications of compliance with the FCC's CPNI rules as required by 47 C.F.R. S: 64.2009(e) for the following affiliated companies:

Hargray Telephone Company, Inc.

Bluffton Telephone Company, Inc.

Hargray Wireless, LLC

Low Country Carriers, Inc., dba Hargray Long Distance

Hargray, Inc.

Hargray of Georgia, Inc.

All inquiries regarding the attached certifications should be directed to my attention at (843) 686-1210.

Sincerely,

Aubrey E. Judy III
Director - Regulatory & Carrier Relations

Attachment

CC: Enforcement Bureau
FCC Copy Service

No. of Copies rec'd 044
List ABCDE

Annual 47 C.F.R. S: 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for [2007]

Date filed: February 29, 2008

Low Country Carriers, Inc.: [LCC]

Form 499 Filer ID: 801399

Name of signatory: Andrew J. Rein

Title of signatory: Secretary & V.P. Finance

I, Andrew J. Rein, certify that I am an officer of Low Country Carriers, Inc., dba Hargray Long Distance, and acting as an agent of LCC, that I have personal knowledge that LCC has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. S: 64.2001 et seq.

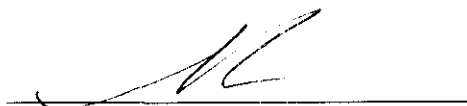
Attached to this certification is an accompanying statement explaining how LCC's procedures ensure that LCC is in compliance with the requirements set forth in section 64.2001 et seq. of the Commission's rules.

LCC has not taken any actions against data brokers in the past year. LCC is aware of one incident by an individual attempting to gain access to CPNI by falsely identifying themselves as a party with a legitimate reason to gain access to such information.

An individual identified himself as a 911 operator and requested the physical address of a wireless customer.

LCC has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed



Received & Inspected

MAR - 3 2008

FCC Mail Room

STATEMENT

Low Country Carriers, Inc. (LCC) has established operating procedures that ensure compliance with the Federal Communication Commission ("Commission") regulations regarding the protection of customer proprietary network information ("CPNI").

- Low Country Carriers, Inc. has implemented a system whereby the status of a customer's CPNI approval can be determined prior to the use of CPNI.
 - LCC sends out an annual opt out notice to its customers as well as a notice to all new customers. This notice is compliant with 64.2008 of the Commission's rules and is maintained for at least one year.
 - LCC maintains an electronic record of the response to these notices for use in determining allowable and non-allowable uses of CPNI. The data is stored in the customer record that appears every time a customer service representative accesses a customer's account.
- Low Country Carriers, Inc. continually educates and trains its employees regarding the appropriate use of CPNI. Low Country Carriers, Inc. has established disciplinary procedures should an employee violate the CPNI procedures established by Low Country Carriers, Inc.
 - LCC has specifically trained all employees that have access to CPNI and provided optional training for all employees. LCC is also creating a training program for new employees regardless of their ability to access CPNI. Both training programs indicate disciplinary actions for improper access to and use of CPNI up to and including dismissal.
- Low Country Carriers, Inc. maintains a record of its and its affiliates' sales and marketing campaigns that use its customers' CPNI. LCC also maintains a record of any and all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record includes a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign. LCC does not plan to share CPNI with 3rd parties. Any instances where LCC uses 3rd parties as part of its marketing efforts, data shared will not include CPNI.
- Low Country Carriers, Inc. has established a supervisory review process regarding compliance with the CPNI rules with respect to outbound marketing situations and maintains records of compliance for a minimum period of one year. Specifically, Low Country Carriers, Inc.'s sales personnel obtain supervisory approval of any proposed outbound marketing request for customer approval regarding its CPNI, and a process ensures that opt-out elections are recorded and followed.

- During 2007, Low Country Carriers, Inc. implemented procedures or confirmed existing procedures for compliance with new Section 64.2010 including, but not limited to the following:
 - Authentication of customers before disclosing CPNI on customer-initiated telephone contacts or business office visits. LCC maintained its existing procedures for authentication of customers for routine activity such as reviewing services provided, questioning specific charges, or adding and removing specific services. In the unusual instance where the customer requests call detail information, we provide that data over the phone only if the customer has a PIN established. If a PIN has not been established, LCC calls the customer back at the designated number, requests that the customer visit the business office and provide photo identification, or mails the information to the address of record.
 - LCC provides customers with on-line access to customer account information controlled by password. LCC previously allowed certain hint questions based on biographical data. When the customer next accessed their account, they received a prompt, which directed them to pick a new question from a list of non-biographical questions.
 - LCC has implemented procedures to provide immediate notification to customers of account changes, including changes in address-of-record and attempts at access to CPNI through use of back-up methods due to forgotten passwords. At this point, however, some of the functionality is not yet active, specifically notification of use of back-up methods due to forgotten passwords. LCC anticipates that it will complete testing and activate all functions within the next thirty (30) days.

Annual 47 C.F.R. S: 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for [2007]

Date filed: February 29, 2008

Hargray of Georgia, Inc.: [HOG]

Form 499 Filer ID: 822722

Name of signatory: Andrew J. Rein

Title of signatory: Secretary & V.P. Finance

I, Andrew J. Rein, certify that I am an officer of Hargray of Georgia, Inc., dba Hargray Long Distance, and acting as an agent of HOG, that I have personal knowledge that HOG has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. S: 64.2001 et seq.

Attached to this certification is an accompanying statement explaining how HOG's procedures ensure that HOG is in compliance with the requirements set forth in section 64.2001 et seq. of the Commission's rules.

HOG has not taken any actions against data brokers in the past year. HOG is aware of one incident by an individual attempting to gain access to CPNI by falsely identifying themselves as a party with a legitimate reason to gain access to such information.

An individual identified himself as a 911 operator and requested the physical address of a wireless customer.

HOG has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed



STATEMENT

Hargray of Georgia, Inc. (HOG) has established operating procedures that ensure compliance with the Federal Communication Commission ("Commission") regulations regarding the protection of customer proprietary network information ("CPNI").

- Hargray of Georgia, Inc. has implemented a system whereby the status of a customer's CPNI approval can be determined prior to the use of CPNI.
 - HOG sends out an annual opt out notice to its customers as well as a notice to all new customers. This notice is compliant with 64.2008 of the Commission's rules and is maintained for at least one year.
 - HOG maintains an electronic record of the response to these notices for use in determining allowable and non-allowable uses of CPNI. The data is stored in the customer record that appears every time a customer service representative accesses a customer's account.
- Hargray of Georgia, Inc. continually educates and trains its employees regarding the appropriate use of CPNI. Hargray of Georgia, Inc. has established disciplinary procedures should an employee violate the CPNI procedures established by Hargray of Georgia, Inc.
 - HOG has specifically trained all employees that have access to CPNI and provided optional training for all employees. HOG is also creating a training program for new employees regardless of their ability to access CPNI. Both training programs indicate disciplinary actions for improper access to and use of CPNI up to and including dismissal.
- Hargray of Georgia, Inc. maintains a record of its and its affiliates' sales and marketing campaigns that use its customers' CPNI. HOG also maintains a record of any and all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record includes a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign. HOG does not plan to share CPNI with 3rd parties. Any instances where HOG uses 3rd parties as part of its marketing efforts, data shared will not include CPNI.
- Hargray of Georgia, Inc. has established a supervisory review process regarding compliance with the CPNI rules with respect to outbound marketing situations and maintains records of compliance for a minimum period of one year. Specifically, Hargray of Georgia, Inc.'s sales personnel obtain supervisory approval of any proposed outbound marketing request for customer approval regarding its CPNI, and a process ensures that opt-out elections are recorded and followed.

- During 2007, Hargray of Georgia, Inc. implemented procedures or confirmed existing procedures for compliance with new Section 64.2010 including, but not limited to the following:
 - Authentication of customers before disclosing CPNI on customer-initiated telephone contacts or business office visits. HOG maintained its existing procedures for authentication of customers for routine activity such as reviewing services provided, questioning specific charges, or adding and removing specific services. In the unusual instance where the customer requests call detail information, we provide that data over the phone only if the customer has a PIN established. If a PIN has not been established, HOG calls the customer back at the designated number, requests that the customer visit the business office and provide photo identification, or mails the information to the address of record.
 - HOG provides customers with on-line access to customer account information controlled by password. HOG previously allowed certain hint questions based on biographical data. When the customer next accessed their account, they received a prompt, which directed them to pick a new question from a list of non-biographical questions.
 - HOG has implemented procedures to provide immediate notification to customers of account changes, including changes in address-of-record and attempts at access to CPNI through use of back-up methods due to forgotten passwords. At this point, however, some of the functionality is not yet active, specifically notification of use of back-up methods due to forgotten passwords. HOG anticipates that it will complete testing and activate all functions within the next thirty (30) days.

Annual 47 C.F.R. S: 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for [2007]

Date filed: February 29, 2008

Hargray Telephone Company: [HTC]

Form 499 Filer ID: 803625

Name of signatory: Andrew J. Rein

Title of signatory: Secretary & V.P. Finance

I, Andrew J. Rein, certify that I am an officer of Hargray Telephone Company, and acting as an agent of HTC, that I have personal knowledge that HTC has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. S: 64.2001 et seq.

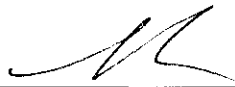
Attached to this certification is an accompanying statement explaining how HTC's procedures ensure that HTC is in compliance with the requirements set forth in section 64.2001 et seq. of the Commission's rules.

HTC has not taken any actions against data brokers in the past year. HTC is aware of one incident by an individual attempting to gain access to CPNI by falsely identifying themselves as a party with a legitimate reason to gain access to such information.

An individual identified himself as a 911 operator and requested the physical address of a wireless customer.

HTC has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed



STATEMENT

Hargray Telephone Company (HTC) has established operating procedures that ensure compliance with the Federal Communication Commission ("Commission") regulations regarding the protection of customer proprietary network information ("CPNI").

- Hargray Telephone Company has implemented a system whereby the status of a customer's CPNI approval can be determined prior to the use of CPNI.
 - HTC sends out an annual opt out notice to its customers as well as a notice to all new customers. This notice is compliant with 64.2008 of the Commission's rules and is maintained for at least one year.
 - HTC maintains an electronic record of the response to these notices for use in determining allowable and non-allowable uses of CPNI. The data is stored in the customer record that appears every time a customer service representative accesses a customer's account.
- Hargray Telephone Company continually educates and trains its employees regarding the appropriate use of CPNI. Hargray Telephone Company has established disciplinary procedures should an employee violate the CPNI procedures established by Hargray Telephone Company.
 - HTC has specifically trained all employees that have access to CPNI and provided optional training for all employees. HTC is also creating a training program for new employees regardless of their ability to access CPNI. Both training programs indicate disciplinary actions for improper access to and use of CPNI up to and including dismissal.
- Hargray Telephone Company maintains a record of its and its affiliates' sales and marketing campaigns that use its customers' CPNI. HTC also maintains a record of any and all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record includes a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign. HTC does not plan to share CPNI with 3rd parties. Any instances where HTC uses 3rd parties as part of its marketing efforts, data shared will not include CPNI.
- Hargray Telephone Company has established a supervisory review process regarding compliance with the CPNI rules with respect to outbound marketing situations and maintains records of compliance for a minimum period of one year. Specifically, Hargray Telephone Company's sales personnel obtain supervisory approval of any proposed outbound marketing request for customer approval regarding its CPNI, and a process ensures that opt-out elections are recorded and followed.

- During 2007, Hargray Telephone Company implemented procedures or confirmed existing procedures for compliance with new Section 64.2010 including, but not limited to the following:
 - Authentication of customers before disclosing CPNI on customer-initiated telephone contacts or business office visits. HTC maintained its existing procedures for authentication of customers for routine activity such as reviewing services provided, questioning specific charges, or adding and removing specific services. In the unusual instance where the customer requests call detail information, we provide that data over the phone only if the customer has a PIN established. If a PIN has not been established, HTC calls the customer back at the designated number, requests that the customer visit the business office and provide photo identification, or mails the information to the address of record.
 - HTC provides customers with on-line access to customer account information controlled by password. HTC previously allowed certain hint questions based on biographical data. When the customer next accessed their account, they received a prompt, which directed them to pick a new question from a list of non-biographical questions.
 - HTC has implemented procedures to provide immediate notification to customers of account changes, including changes in address-of-record and attempts at access to CPNI through use of back-up methods due to forgotten passwords. At this point, however, some of the functionality is not yet active, specifically notification of use of back-up methods due to forgotten passwords. HTC anticipates that it will complete testing and activate all functions within the next thirty (30) days.

Annual 47 C.F.R. S: 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for [2007]

Date filed: February 29, 2008

Hargray Wireless, LLC: [HW]

Form 499 Filer ID: 818108

Name of signatory: Andrew J. Rein

Title of signatory: Secretary & V.P. Finance

I, Andrew J. Rein, certify that I am an officer of Hargray Wireless, LLC, and acting as an agent of HW, that I have personal knowledge that HW has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. S: 64.2001 et seq.

Attached to this certification is an accompanying statement explaining how HW's procedures ensure that HW is in compliance with the requirements set forth in section 64.2001 et seq. of the Commission's rules.

HW has not taken any actions against data brokers in the past year. HW is aware of one incident by an individual attempting to gain access to CPNI by falsely identifying themselves as a party with a legitimate reason to gain access to such information.

An individual identified himself as a 911 operator and requested the physical address of a wireless customer.

HW has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed



STATEMENT

Hargray Wireless, LLC (HW) has established operating procedures that ensure compliance with the Federal Communication Commission (“Commission”) regulations regarding the protection of customer proprietary network information (“CPNI”).

- Hargray Wireless, LLC has implemented a system whereby the status of a customer’s CPNI approval can be determined prior to the use of CPNI.
 - HW sends out an annual opt out notice to its customers as well as a notice to all new customers. This notice is compliant with 64.2008 of the Commission’s rules and is maintained for at least one year.
 - HW maintains an electronic record of the response to these notices for use in determining allowable and non-allowable uses of CPNI. The data is stored in the customer record that appears every time a customer service representative accesses a customer’s account.
- Hargray Wireless, LLC continually educates and trains its employees regarding the appropriate use of CPNI. Hargray Wireless, LLC has established disciplinary procedures should an employee violate the CPNI procedures established by Hargray Wireless, LLC.
 - HW has specifically trained all employees that have access to CPNI and provided optional training for all employees. HW is also creating a training program for new employees regardless of their ability to access CPNI. Both training programs indicate disciplinary actions for improper access to and use of CPNI up to and including dismissal.
- Hargray Wireless, LLC maintains a record of its and its affiliates' sales and marketing campaigns that use its customers' CPNI. HW also maintains a record of any and all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record includes a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign. HW does not plan to share CPNI with 3rd parties. Any instances where HW uses 3rd parties as part of its marketing efforts, data shared will not include CPNI.
- Hargray Wireless, LLC has established a supervisory review process regarding compliance with the CPNI rules with respect to outbound marketing situations and maintains records of compliance for a minimum period of one year. Specifically, Hargray Wireless, LLC’s sales personnel obtain supervisory approval of any proposed outbound marketing request for customer approval regarding its CPNI, and a process ensures that opt-out elections are recorded and followed.

- During 2007, Hargray Wireless, LLC implemented procedures or confirmed existing procedures for compliance with new Section 64.2010 including, but not limited to the following:
 - Authentication of customers before disclosing CPNI on customer-initiated telephone contacts or business office visits. HW maintained its existing procedures for authentication of customers for routine activity such as reviewing services provided, questioning specific charges, or adding and removing specific services. In the unusual instance where the customer requests call detail information, we provide that data over the phone only if the customer has a PIN established. If a PIN has not been established, HW calls the customer back at the designated number, requests that the customer visit the business office and provide photo identification, or mails the information to the address of record.
 - HW provides customers with on-line access to customer account information controlled by password. HW previously allowed certain hint questions based on biographical data. When the customer next accessed their account, they received a prompt, which directed them to pick a new question from a list of non-biographical questions.
 - HW has implemented procedures to provide immediate notification to customers of account changes, including changes in address-of-record and attempts at access to CPNI through use of back-up methods due to forgotten passwords. At this point, however, some of the functionality is not yet active, specifically notification of use of back-up methods due to forgotten passwords. HW anticipates that it will complete testing and activate all functions within the next thirty (30) days.

Annual 47 C.F.R. S: 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for [2007]

Date filed: February 29, 2008

Bluffton Telephone Company: [BTC]

Form 499 Filer ID: 806109

Name of signatory: Andrew J. Rein

Title of signatory: Secretary & V.P. Finance

I, Andrew J. Rein, certify that I am an officer of Bluffton Telephone Company, and acting as an agent of BTC, that I have personal knowledge that BTC has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. S: 64.2001 et seq.

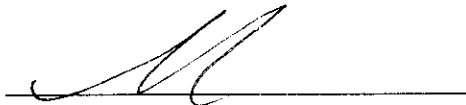
Attached to this certification is an accompanying statement explaining how BTC's procedures ensure that BTC is in compliance with the requirements set forth in section 64.2001 et seq. of the Commission's rules.

BTC has not taken any actions against data brokers in the past year. BTC is aware of one incident by an individual attempting to gain access to CPNI by falsely identifying themselves as a party with a legitimate reason to gain access to such information.

An individual identified himself as a 911 operator and requested the physical address of a wireless customer.

BTC has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed

A handwritten signature in black ink, appearing to be 'A. Rein', is written over a horizontal line.

STATEMENT

Bluffton Telephone Company (BTC) has established operating procedures that ensure compliance with the Federal Communication Commission ("Commission") regulations regarding the protection of customer proprietary network information ("CPNI").

- Bluffton Telephone Company has implemented a system whereby the status of a customer's CPNI approval can be determined prior to the use of CPNI.
 - BTC sends out an annual opt out notice to its customers as well as a notice to all new customers. This notice is compliant with 64.2008 of the Commission's rules and is maintained for at least one year.
 - BTC maintains an electronic record of the response to these notices for use in determining allowable and non-allowable uses of CPNI. The data is stored in the customer record that appears every time a customer service representative accesses a customer's account.
- Bluffton Telephone Company continually educates and trains its employees regarding the appropriate use of CPNI. Bluffton Telephone Company has established disciplinary procedures should an employee violate the CPNI procedures established by Bluffton Telephone Company.
 - BTC has specifically trained all employees that have access to CPNI and provided optional training for all employees. BTC is also creating a training program for new employees regardless of their ability to access CPNI. Both training programs indicate disciplinary actions for improper access to and use of CPNI up to and including dismissal.
- Bluffton Telephone Company maintains a record of its and its affiliates' sales and marketing campaigns that use its customers' CPNI. BTC also maintains a record of any and all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record includes a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign. BTC does not plan to share CPNI with 3rd parties. Any instances where BTC uses 3rd parties as part of its marketing efforts, data shared will not include CPNI.
- Bluffton Telephone Company has established a supervisory review process regarding compliance with the CPNI rules with respect to outbound marketing situations and maintains records of compliance for a minimum period of one year. Specifically, Bluffton Telephone Company's sales personnel obtain supervisory approval of any proposed outbound marketing request for customer approval regarding its CPNI, and a process ensures that opt-out elections are recorded and followed.

- During 2007, Bluffton Telephone Company implemented procedures or confirmed existing procedures for compliance with new Section 64.2010 including, but not limited to the following:
 - Authentication of customers before disclosing CPNI on customer-initiated telephone contacts or business office visits. BTC maintained its existing procedures for authentication of customers for routine activity such as reviewing services provided, questioning specific charges, or adding and removing specific services. In the unusual instance where the customer requests call detail information, we provide that data over the phone only if the customer has a PIN established. If a PIN has not been established, BTC calls the customer back at the designated number, requests that the customer visit the business office and provide photo identification, or mails the information to the address of record.
 - BTC provides customers with on-line access to customer account information controlled by password. BTC previously allowed certain hint questions based on biographical data. When the customer next accessed their account, they received a prompt, which directed them to pick a new question from a list of non-biographical questions.
 - BTC has implemented procedures to provide immediate notification to customers of account changes, including changes in address-of-record and attempts at access to CPNI through use of back-up methods due to forgotten passwords. At this point, however, some of the functionality is not yet active, specifically notification of use of back-up methods due to forgotten passwords. BTC anticipates that it will complete testing and activate all functions within the next thirty (30) days.

Annual 47 C.F.R. S: 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for [2007]

Date filed: February 29, 2008

Hargray, Inc.: [HI]

Form 499 Filer ID: 821672

Name of signatory: Andrew J. Rein

Title of signatory: Secretary & V.P. Finance

I, Andrew J. Rein, certify that I am an officer of Hargray, Inc., and acting as an agent of HI, that I have personal knowledge that HI has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. S: 64.2001 et seq.


Attached to this certification is an accompanying statement explaining how HI's procedures ensure that HI is in compliance with the requirements set forth in section 64.2001 et seq. of the Commission's rules.

HI has not taken any actions against data brokers in the past year. HI is aware of one incident by an individual attempting to gain access to CPNI by falsely identifying themselves as a party with a legitimate reason to gain access to such information.

An individual identified himself as a 911 operator and requested the physical address of a wireless customer.

HI has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed



STATEMENT

Hargray, Inc. (HI) has established operating procedures that ensure compliance with the Federal Communication Commission ("Commission") regulations regarding the protection of customer proprietary network information ("CPNI").

- Hargray, Inc. has implemented a system whereby the status of a customer's CPNI approval can be determined prior to the use of CPNI.
 - HI sends out an annual opt out notice to its customers as well as a notice to all new customers. This notice is compliant with 64.2008 of the Commission's rules and is maintained for at least one year.
 - HI maintains an electronic record of the response to these notices for use in determining allowable and non-allowable uses of CPNI. The data is stored in the customer record that appears every time a customer service representative accesses a customer's account.
- Hargray, Inc. continually educates and trains its employees regarding the appropriate use of CPNI. Hargray, Inc. has established disciplinary procedures should an employee violate the CPNI procedures established by Hargray, Inc.
 - HI has specifically trained all employees that have access to CPNI and provided optional training for all employees. HI is also creating a training program for new employees regardless of their ability to access CPNI. Both training programs indicate disciplinary actions for improper access to and use of CPNI up to and including dismissal.
- Hargray, Inc. maintains a record of its and its affiliates' sales and marketing campaigns that use its customers' CPNI. HI also maintains a record of any and all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record includes a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign. HI does not plan to share CPNI with 3rd parties. Any instances where HI uses 3rd parties as part of its marketing efforts, data shared will not include CPNI.
- Hargray, Inc. has established a supervisory review process regarding compliance with the CPNI rules with respect to outbound marketing situations and maintains records of compliance for a minimum period of one year. Specifically, Hargray, Inc.'s sales personnel obtain supervisory approval of any proposed outbound marketing request for customer approval regarding its CPNI, and a process ensures that opt-out elections are recorded and followed.
- During 2007, Hargray, Inc. implemented procedures or confirmed existing procedures for compliance with new Section 64.2010 including, but not limited to the following:

- Authentication of customers before disclosing CPNI on customer-initiated telephone contacts or business office visits. HI maintained its existing procedures for authentication of customers for routine activity such as reviewing services provided, questioning specific charges, or adding and removing specific services. In the unusual instance where the customer requests call detail information, we provide that data over the phone only if the customer has a PIN established. If a PIN has not been established, HI calls the customer back at the designated number, requests that the customer visit the business office and provide photo identification, or mails the information to the address of record.
- HI provides customers with on-line access to customer account information controlled by password. HI previously allowed certain hint questions based on biographical data. When the customer next accessed their account, they received a prompt, which directed them to pick a new question from a list of non-biographical questions.
- HI has implemented procedures to provide immediate notification to customers of account changes, including changes in address-of-record and attempts at access to CPNI through use of back-up methods due to forgotten passwords. At this point, however, some of the functionality is not yet active, specifically notification of use of back-up methods due to forgotten passwords. HI anticipates that it will complete testing and activate all functions within the next thirty (30) days.